GeoPlatform

GIS Cloud Hosting Security Rules of Behavior

As the owner or administrator of services and/or applications deployed in the GeoPlatform Cloud Hosting environment, I understand and acknowledge that although the service and/or application is deployed in the Amazon Web Service (AWS) environment, the same Federal information security requirements apply as if this service and/or application was deployed on the DOI network. Additionally, I acknowledge and agree to the following information security requirements:

All documents referenced in this Security Rules of Behavior are also located in the GeoPlatform Customers community onboarding page https://communities.geoplatform.gov/gpcustomers/.

Please submit all required documents to GIS Cloud Hosting Services

1. Submit the completed DOI FIPS 199 Workbook. Verify that the data types are appropriate at FISMA LOW or MODERATE for use on the GeoPlatform.
2. Sign the *GIS Cloud Hosting Security Rules of Behavior* document prior to being granted access to the hosting environment.
3. Submit the GIS Service and Application spreadsheet. List all public facing applications and services. There is no requirement to list sandbox or dev environments.
4. Read and follow the customer responsibilities as documented in the Customer Responsibility Matrix.
5. Notify via email within 5 business days of a change to any of the following:
    - Information and/or Information Types
    - Addition or Removal of application/service from initial list of applications/services provided
    - Application Owner in this *GIS Cloud Hosting Security Rules of Behavior*.
6. Participate in the security assessment, security authorization, and continuous monitoring by providing information and/or taking specific action(s) as instructed by the Security Manager.
7. Utilize application level scanning tools to conduct application scans according to your Bureau/ Agency requirements.
8. Remediate any legitimate application/service weaknesses found through vulnerability scanning as follows:
    - Public facing
        - Critical/High Severity weaknesses mitigated within 30 days from date of discovery;
        - Moderate Severity weaknesses mitigated within 60 days from date of discovery;
        - Low severity weaknesses mitigated within 90 days from date of discovery;

9. Ensure the application/service has been incorporated into either an existing or a new Information System Contingency Plan (ISCP) that provides for recovery of the applications/service, within the allowable downtime identified in the local Business Impact Analysis, and conducts annual testing and training of the ISCP. The ISCP testing should be performed in conjunction with the Incident Response testing. The Recovery Time Objective (RTO) should be documented and communicated to the GeoPlatform System Owner (SO).

10. The GIS cloud hosting services provided by Zivaro will include backups as part of the cloud hosted services. GeoPlatform applications, however, are not provided with backups of applications deployed.

11. Deploy the application/service using only hardened images, stacks or instances provided and approved by the GeoPlatform team. Any legitimate need to deviate from the standard instances will be considered case by case.

12. Use application/service software only in accordance with contract agreements and copyright laws, and track use of such software.

13. Configure application level auditing as follows:

    - Generate audit records containing information that establishes: what type of event occurred, when the event occurred, where the event occurred, source of the event, outcome of the event, and identity of subjects associated with the event; and
    - Review and analyze audit records at least weekly for indications of organization-defined inappropriate or unusual activity; and
    - Retain such audit records for 90 days; and
    - Protect audit records from unauthorized access, modification and deletion.

14. For any publicly available application/service in the GeoPlatform:

    - Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that non-public information is not included;
    - Review the content on the publicly accessible information system for non-public information at least quarterly and remove such information if discovered.
    - Check the validity of information inputs (if any);
    - Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries
    - Reveal error messages only to authorized personnel.

15. Ensure proper handling and disposition of information within the application/service through either a new or existing file plan that covers the identification, access, handling, and disposition of records in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.


GeoPlatform

GIS Cloud Hosting Security Rules of Behavior

16. If at any time there is an indication that a security incident has occurred (e.g. server compromise or virus infection), the incident will be reported immediately via email to the following recipients:
    - GeoPlatform Security Manager
    - gp_doi_hosting@geoplatform.gov
    - DOI Computer Security Incident Response Team

The GeoPlatform ATO was signed on 16 January 2018 and is valid for 5 years; provided that the following caveats are met/maintained:

1. Vulnerability scan reports are provided on the 15th of each month.
2. Plan of Action and Milestones (POA&M) are provided on the 15th of each quarter (January, April, July, and October).
3. Contingency Plan, Incident Response Plan and Test Report, IT Security Awareness Training, IT Security Policies, Physical Access Inventory, Configuration Management Plan, IT Contingency Plan & Test Report, Separation of Duties Matrix, and System Security Plan are provided on the ATO anniversary date each year (16 January) during the 5 year ATO period.
4. The vulnerabilities reported do not result in additional risk which is deemed unacceptable by the Authorizing Official.

Additionally, Information System Owners are responsible for documenting proposed or actual changes to the information system and its operating environment and determining the impact of those changes on the overall secure state of the system. Information System Owners must take appropriate action to maintain a level of assurance consistent with this authorization. The System Security Plan, IT Contingency and Disaster Response Plan, Incident Response Plan, Security Assessment Report, and Plan of Action and Milestones report shall be updated as necessary. System status/changes will be reported to the Authorizing Official on an ongoing basis and during quarterly reviews of the status of corrective actions of weaknesses documented in the Plan of Action and Milestones (POA&M).

I have read, understand, and agree to abide by the *Geospatial Cloud Hosting Security Rules of Behavior*. I understand that failure to abide by these rules of behavior may result in termination of the service or application.

Name: _____

Signature: _____

Date: _____

(Retain a copy of your signed Rules of Behavior for your records and provide the original, signed copy to the Security Manager.)